Guía de divulgación de **incidentes** de **seguridad digital**

(para periodistas)





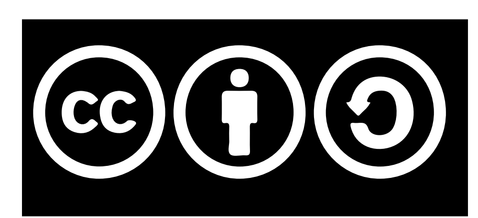
Participación cívica



Bogotá, Colombia, febrero 2024

20 años Fundación Karisma

En un esfuerzo para que todas las personas tengan acceso al conocimiento, la Fundación Karisma está trabajando para que sus documentos sean accesibles. Esto quiere decir que su formato incluye metadatos y otros elementos que lo hacen compatible con herramientas como lectores de pantalla o pantallas braille. El propósito del diseño accesible es que todas las personas, incluidas las que tienen algún tipo de discapacidad o dificultad para la lectura y comprensión, puedan acceder a los contenidos.



Contenido

Introducción

Para cualquier persona -y en particular para periodistas, funcionarias del sector público o activistas- dar a conocer incidentes de seguridad digital es un gran reto y responsabilidad. No hacerlo correctamente puede poner en peligro a las personas, a la información de las mismas o a los sistemas que les prestan servicios esenciales como los de salud, transporte o energía. Por el contrario, hacer una divulgación responsable ayuda tanto a una mejor resolución del problema, como a extender la cultura y el conocimiento en seguridad digital y a incrementar la transparencia frente al incidente.

El propósito de esta guía que hemos elaborado desde el Laboratorio de Seguridad Digital y Privacidad (K+Lab) y la línea de Participación Cívica de Fundación Karisma es compartir algunas recomendaciones prácticas para periodistas y para otras personas interesadas en divulgar vulnerabilidades y reportar incidentes de seguridad digital. Esta guía nace del trabajo de incidencia e investigación de Karisma sobre la política de ciberseguridad y de una serie de talleres realizados con periodistas que cubren tecnología y seguridad digital.

Creemos que mejorar las capacidades y conocimientos para cubrir estos temas tendrá un impacto en la sociedad en general y servirá para contribuir a la generación de confianza, a fortalecer los mecanismos de acceso a la información sin caer en la generación de miedo, y a disminuir la propagación de desinformación en escenarios donde los incidentes son de interés general.

¿Qué es un incidente de seguridad digital?

A nivel internacional se entiende por incidente un evento o una serie de eventos de seguridad digital no deseados o no esperados y que tienen una probabilidad significativa de comprometer las actividades y de amenazar la seguridad de la información en su disponibilidad, su integridad o su confidencialidad.

El Ministerio de las Tecnologías de la Información y las comunicaciones (MinTIC) define los incidentes utilizando los siguiente ejemplos:

"un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o una violación a una Política de **Seguridad** de la Información".



En seguridad digital se habla de tres propiedades básicas que deben mantenerse para preservar la información: disponibilidad, integridad y confidencialidad, vinculadas, además, con la necesidad de autenticación. En consecuencia, se pueden identificar **seis clases de incidentes de seguridad digital** según las propiedades afectadas en el suceso:

1. No disponibilidad temporal de un recurso. Hablamos de la falta de acceso oportuno a los datos o recursos (sitios web, aplicaciones, redes, servidores o equipos). La no disponibilidad se traduce en la imposibilidad de ingresar a un sitio o acceder a cierta información. Esto se puede dar debido a una falla técnica, un error humano o a un ataque intencionado.

›Ejemplo: *la caída de un sitio web por un ataque de denegación de servicio, como lo que le sucedió a ChatGPT en noviembre de 2023 o la caída de los servicios de WhatsApp e Instagram en octubre de 2021 debido a errores técnicos en cambios de configuración.*

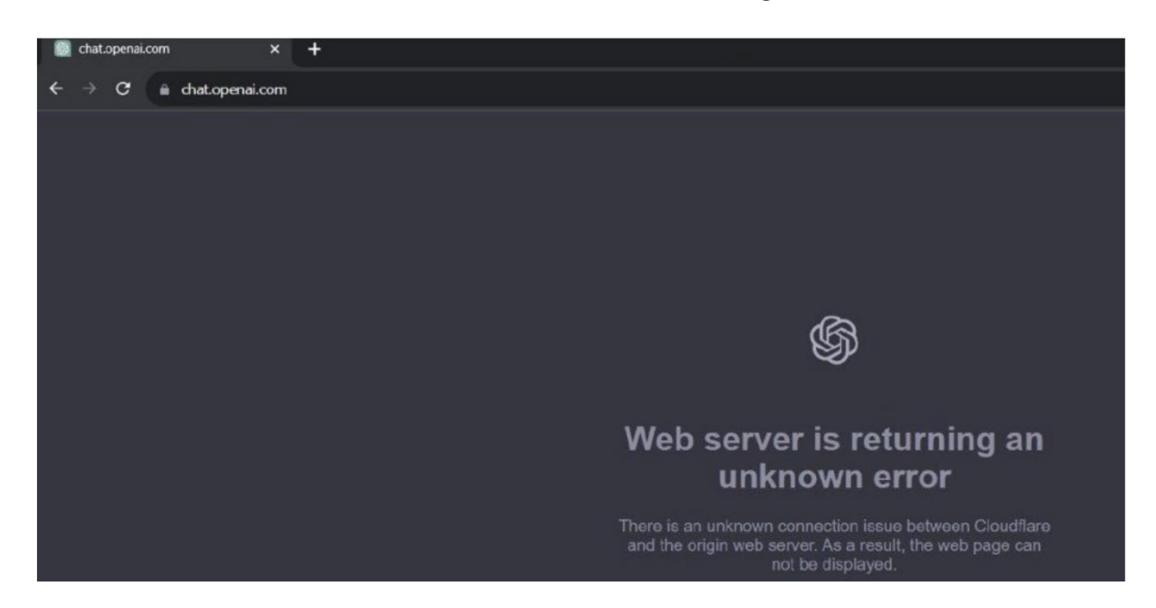


Imagen del error que se mostraba durante el ataque de denegación de servicios a OpenIA y que afectó temporalmente el acceso a los servicios de CharGPT. Fuente: https://www.hackread.com/chatgpt-down-openai-ddos-attacks-outages/

2. No disponibilidad con pérdida temporal o definitiva de datos. Se presenta cuando hay una afectación a los datos que genera en consecuencia falta de disponibilidad. La información almacenada en el sistema se compromete y su recuperación no siempre es posible.

La pérdida de datos implica la corrupción (introducción de cambios no deseados), sustracción o eliminación de la información almacenada, con lo que eventualmente se compromete su integridad.

›Ejemplo: *El ataque de ransomware, que cifró los datos de Keralty a finales de 2022. En este caso, los servicios de salud prestado por la EPS Sanitas y medicina prepagada de Colsanitas y Medisanitas se vieron afectados por la imposibilidad de acceder a historias clínicas, información de procedimientos y otros datos almacenados en sus sistemas que resultaron cifrados por el ataque. La recuperación plena de los servicios tomó semanas.*

3. Modificación de un recurso. Sucede cuando de forma intencionada se accede a los servidores de una entidad y se cambia la información que estas comparten de manera pública. En general estos ataques no comprometen la información alojada en el servidor, pero pero sí ponen de manifiesto vulnerabilidades en la infraestructura. Se pueden considerar como ataques reputacionales.

›Ejemplo: *Los ataques de "defacement" (cambio de la información visible en un sitio web) realizados por hacktivistas con el objetivo de llamar la atención sobre un asunto de interés público. En Colombia esta modalidad se hizo famosa en 2011 cuando Anonymous modificó la información que se mostraba en la página del Senado de la República en oposición a la ley Lleras. Estos ataques luego se invocaron en la creación de la primera política pública sobre ciberseguridad y ciberdefensa, el Conpes 3701.*



Captura de imagen del sitio web del Senado de la República durante el ataque de defacement realizado por Anonymous en 2011 como parte de su protesta en contra de la Ley Lleras. Fuente: Imagen de archivo

4. Fuga de datos personales y no personales. Se da cuando terceros tienen acceso no autorizado a la información que almacenan sitios web, bases de datos o servidores. Este acceso se puede generar por problemas de vulnerabilidades o fallas de los sistemas. También porque se sobrepasan las barreras de protección dispuestas por el sitio de forma intencional.

***›Ejemplo:** La vulnerabilidad en la página web de Cancillería que permitía acceder, sin autorización a los datos de las visas de las personas ciudadanas extranjeras en Colombia. Este caso fue expuesto por La Silla Vacía y, si bien fue solucionado por la entidad, también es un ejemplo de la necesidad que existe de que los medios de comunicación mejoren sus capacidades y conocimientos para reportar esta clase de incidentes, ya que en el artículo se exponía innecesariamente una vulnerabilidad que podía ser explotada con peores consecuencias.*

***Otro ejemplo** fueron las primeras versiones de Coronapp Colombia en las que algunas personas investigadoras de seguridad digital encontraron que había una vulnerabilidad que permitía un escenario de fuga de información. El problema era tal, que era posible para un*

atacante, no muy sofisticado, filtrar total o parcialmente la base de datos de la aplicación.

Esta vulnerabilidad, muy fácilmente se hubiera podido volver una fuga de datos.

La Silla Vacía.

NACIONAL

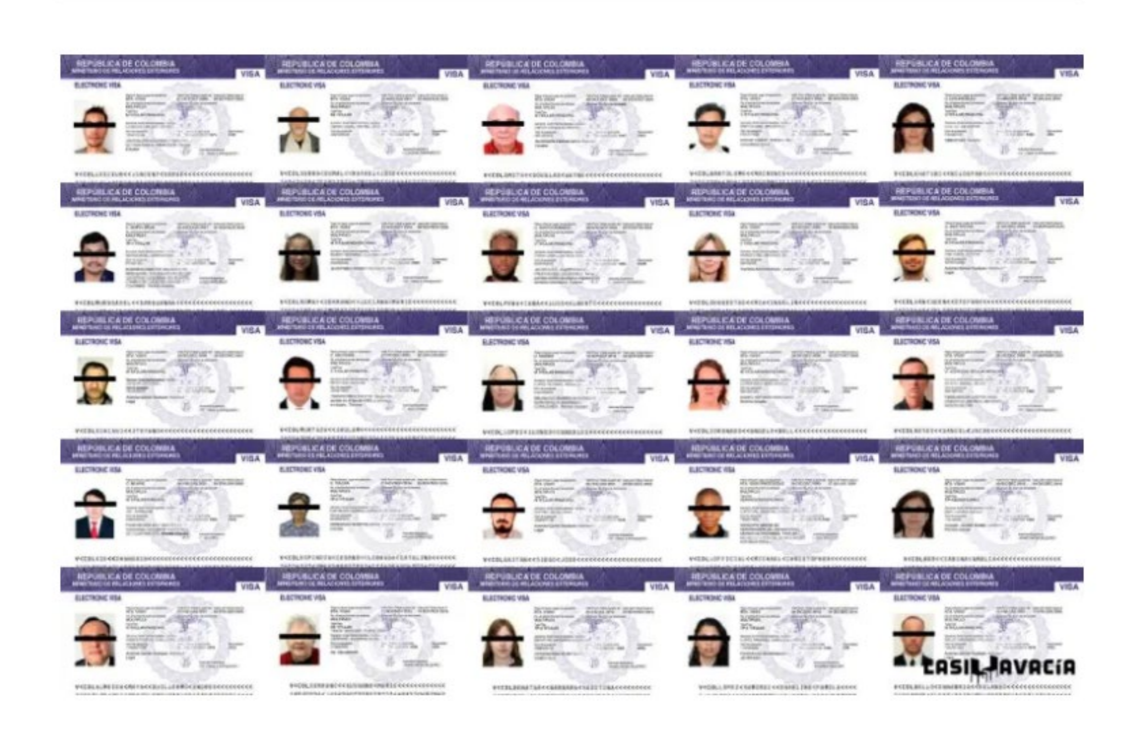
UN BACHE DE SEGURIDAD AMENAZÓ LOS DATOS DE EXTRANJE-ROS Y CANCILLERÍA NO SABÍA

Por **Tatiana Duque**

enero 15, 2021





Captura de imagen del artículo de La silla vacía sobre el caso de la fuga de datos de Cancillería.
Fuente: Imagen de archivo

5. Uso no autorizado de recursos con propósito fraudulento. Cuando se utiliza el incidente para obtener un beneficio económico a través de una actividad ilegal.

›Ejemplo: Es frecuente que servidores y sitios web que no han sido actualizados sean utilizados para realizar actividades ilegales. Por ejemplo, hacer ataques de denegación de servicios a otros sitios, ofrecer productos ilícitos o fraudulentos en un sitio web, insertar publicidad maliciosa o enviar correos de phishing.

6. Intrusión o ataque sin fuga de datos o uso fraudulento. Cuando alguien se introduce en un sistema pero no hay robo de datos o alteración del sistema con fines fraudulentos.

›Ejemplos: Esto puede pasar en las fases de reconocimiento previos a un futuro ataque, cuando la persona atacante no logra ir hacia su meta final (superó algunas barreras de protección pero no todas) o si sólo quiso mostrar que “puede entrar” o simplemente se quedó observando y estudiando el servidor. Es importante estar en capacidad de detectar estos eventos también para evitar daños posteriores. Es poco común que estos ataques se hagan públicos.

Consideraciones esenciales para cubrir incidentes de seguridad digital

La Organización para la Cooperación y el Desarrollo Económico (OCDE) ha emitido una serie de guías y recomendaciones para pensar y generar políticas públicas de seguridad digital. Algunas de estas recomendaciones se adaptan bien al oficio periodístico y abordan temas que se deben tener en cuenta al momento de cubrir un incidente. Aquí les dejamos algunas:

- **No se debe olvidar que los incidentes pueden tener distintos orígenes.** Un incidente puede provenir de una acción intencionada (ataque) o no intencionada (errores humanos, problemas de infraestructura o fenómenos naturales). Cuando los incidentes son intencionados, estos pueden ser ocasionados por individuos sin muchas capacidades técnicas, organizaciones criminales poderosas con grandes capacidades y hasta por instituciones vinculadas a los estados.

- **Los causantes de un incidente pueden tener distintas motivaciones.** Desde objetivos geopolíticos (cuando se trata de ataques apoyados por los estados), pasando por los puramente económicos (los ransomware extorsivos adelantados por bandas criminales), hasta los que persiguen objetivos ideológicos como aquellos vinculados con actividades de "hacktivistas".

- **En muchos casos es difícil identificar a la persona atacante o la modalidad de ataque solo por la forma en que operaron.** Por ejemplo, es posible que un atacante que está actuando en nombre de un estado use los métodos de atacantes con finalidades económicas solo para encubrir sus intenciones. Tenga cuidado al atribuir responsabilidades. Informar sobre el origen y las motivaciones cuando están establecidas y no especular sobre estas, ayuda a clarificar la situación y no generar alertas innecesarias.

- **Se debe evaluar el contexto de cada caso.** Un incidente puede haberse concretado por la presencia de distintas vulnerabilidades, pero también por la búsqueda y explotación de vulnerabilidades no conocidas. Es posible que se pueda identificar diferentes factores que hayan contribuido a materializar un incidente, desde los humanos (por ejemplo que quien administra no tenga suficientes conocimientos para proteger un sistema), institucionales (como cuando una organización no tiene políticas sobre copias de respaldo o recursos para hacerlas) y hasta tecnológicos (como vulnerabilidades no conocidas presentes en el código del software).

- **Antes de atribuir responsabilidad** o señalar culpables recuerde que un incidente de seguridad digital suele estar causado por un conjunto de factores, que incluye la falta de toma de decisión pero también la falta de recursos para implementar mejoras. Es complejo atribuir responsabilidad sin tener en cuenta las acciones y omisiones de todas las personas involucradas.

- **Verifique la información antes de publicar.** Intente utilizar información directamente obtenida de las fuentes o de comunicados oficiales. Revisé las cuentas en redes sociales y los sitios oficiales, llame directamente a la entidad o empresa. Tenga en cuenta que la información errónea puede generar falsos rumores o pánico.

- **Tenga en cuenta que tanto la investigación en este tema como la publicación puede ser jurídicamente riesgosa.** Algunas autoridades pueden considerar actividades relacionadas con la reportería o la investigación de seguridad digital, como el ingreso a un sistema o la difusión o posesión de información relacionada con la seguridad nacional, un delito. Busque asesoría jurídica experta en su país.

Recomendaciones para el cubrimiento de incidentes con fuga de datos de acceso público

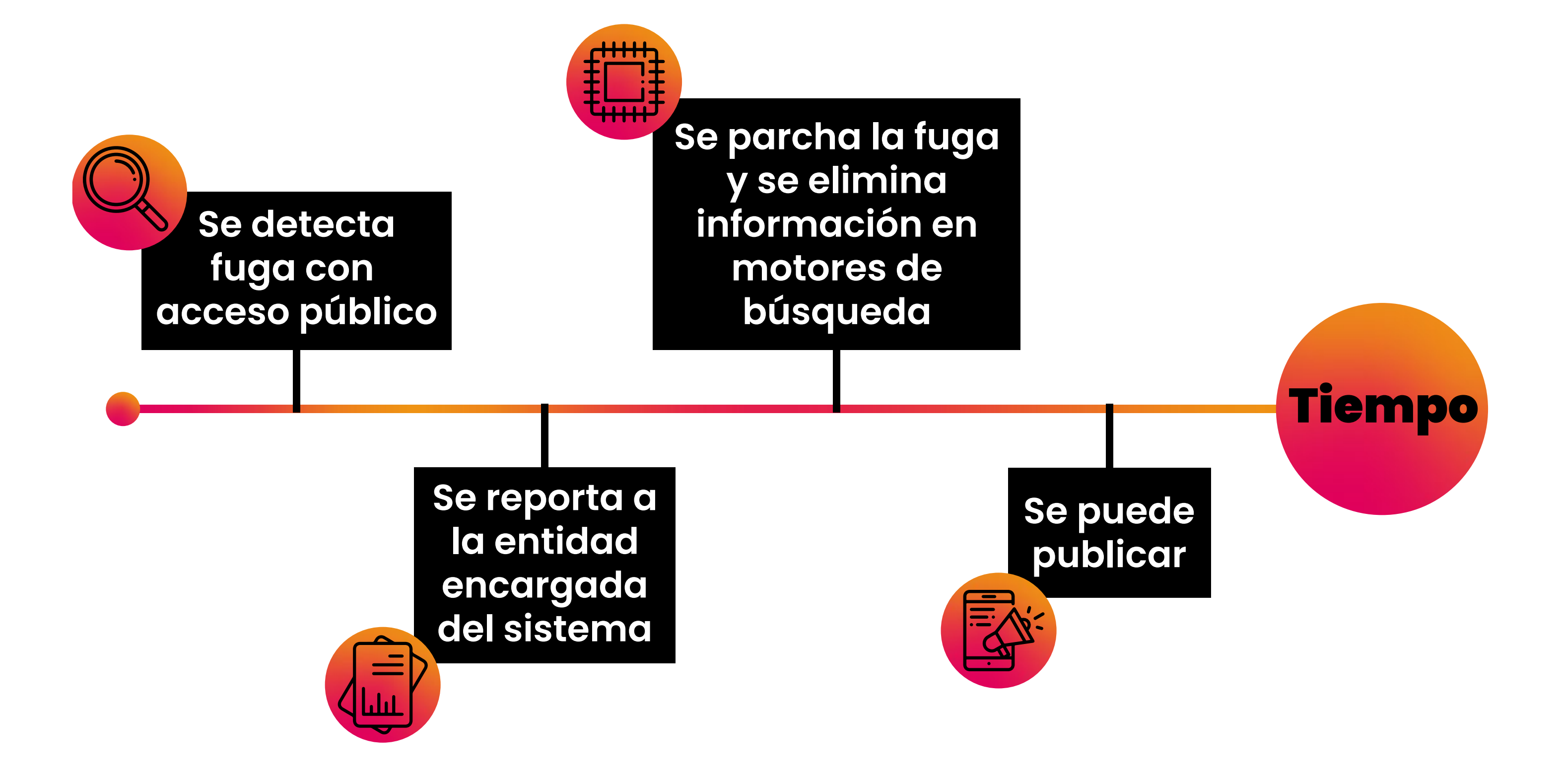
Algunos incidentes de ciberseguridad dejan expuesta información sensible de la ciudadanía. Es decir, que al descubrirse o usarse una vulnerabilidad de un sistema es posible ver, descargar, alterar o eliminar información relacionada con la privacidad de las personas (dirección o información médica, por ejemplo) o con base en la cuál puede ser discriminada (creencias religiosas o filiación política, por ejemplo). En casos así, es fundamental no exponer la fuga de datos, no publicar y explicar cómo acceder a la misma, antes de que el sistema sea arreglado (parchado). De lo contrario, se difundirá información con la cual terceros, mal intencionados o no, puedan acceder a datos de miles o millones de ciudadanos.

Teniendo esto en cuenta, para informar sobre casos de fuga de datos recomendamos que:

1. Tenga cuidado al realizar la reportería para verificar una fuga de datos. El acceso no autorizado a un sistema informático es un delito en casi todos los países de la región. Recuerde que si una puerta está entreabierta o no tiene cerradura no implica que sea legal entrar a una casa.

2. Verifique si la entidad tiene conocimiento del incidente. Hablar con la entidad atacada le permitirá verificar información y alertará a la víctima para que tome las medidas adecuadas en caso de no estar al tanto.

3. No reporte con detalles (sistema, entidad y forma de explotación de una vulnerabilidad) que puedan facilitar el acceso mientras la brecha de seguridad no esté cerrada. Recuerde que la información a la que se puede acceder puede caer en manos equivocadas.



Recomendaciones en caso de otros incidentes

(no disponibilidad, modificación de sistema, etc.)

Existen otros tipos de incidentes como por ejemplo la caída de un sistema o su alteración. Entender lo que ha pasado y hacer una publicación responsable al respecto no siempre es fácil. Por esto recomendamos que:

1. Diversifique las fuentes y contraste la información para evitar generar desinformación o pánico. Consulte con las entidades víctimas del ataque, hable con los equipos de respuesta a incidentes del Estado, con los responsables de la política pública de ciberseguridad y con los expertos y expertas independientes. Busque información en páginas y cuentas oficiales. Hablar con múltiples partes evitará que reproduzca información falsa o que reporte falsos incidentes como sucedió con el Ejército durante el Paro Nacional de 2021 o con la Registraduría durante las elecciones de 2022.

2. Incluya un enfoque humano al reportar un incidente de ciberseguridad. Las víctimas no son culpables y suelen estar bajo mucha presión tras el ataque. Sea cuidadoso al atribuir culpas, a cualquiera le puede pasar.

3. Intente ser lo más claro posible. En muchas ocasiones será necesario presentar definiciones, usar ejemplos e incluir el contexto para poder dar cuenta de la complejidad de un incidente.

Recomendaciones en caso de filtraciones (*leaks*)

Un incidente de seguridad digital puede concluir con la fuga de información de interés público que es filtrada a la prensa (es el caso de los Panama Papers o los Guacamaya Leaks).

Con frecuencia los y las periodistas obtienen información filtrada que todavía no es de conocimiento público y cuya divulgación puede entrañar riesgos que deben ser analizados antes de publicar. Para este propósito recomendamoscomo mínimo considerar lo siguiente:

1. Recuerde que en las actividades de reportería, las personas con las que habla, los documentos usados y la forma que los obtuvo están protegidos por el secreto de la fuente, un estándar interamericano. Sin embargo, revise su legislación nacional y asesórese con una persona experta para disminuir riesgos jurídicos. En caso de recibir presión para revelar sus fuentes, recuerde que no tiene la obligación a hacerlo.

2. Las filtraciones o leaks pueden incluir cantidades gigantescas de información. Antes de acceder y almacenar esta información tome medidas de seguridad y adquiera las herramientas y capacidades necesarias para manejar esa información (Usar una VPN o TOR para descargar la información, almacenar la descarga en

un disco duro encriptado, etc.).

3. Asegure la integridad de la información. Recuerde que los documentos pudieron ser alterados antes de llegar a usted o que pueden existir varias versiones de un mismo documento. El mejor mecanismos para llevar cuenta de la trazabilidad e integridad de los archivos es revisar su HASH[1]. Este es un código único que permite verificar la integridad de un documento y que varía cuando se hace un cambio en el mismo.

4. No transporte la información si no es necesario y - si el tamaño de la información lo permite - tenga dos copias. Esto ayuda a preservar la información y también permite confirmar su integridad de ser necesario. Tenga en cuenta que si la información es sensible, al transportarla puede perderla o una autoridad puede encontrarla en su poder.

5. Tenga en cuenta que una filtración o leak incluye información de terceros. Si esta información hace parte del derecho a la intimidad de terceros o puede ser información que comprometa la seguridad digital de la ciudadanía. Divulgar esta información puede tener consecuencias jurídicas para la persona periodista o de otra índole para las personas a las que se refiere (como por ejemplo lo que significa revelar la identidad de agentes de inteligencia en operaciones encubiertas).

6. Contraste y verifique la información de las filtraciones o leaks. Los deberes de imparcialidad y veracidad aplican (por ejemplo, la información puede estar desactualizada).

7. Analice con una persona abogada local los riesgos que en su jurisdicción entraña tener información relacionada con seguridad nacional (si es que la filtración tiene información en esa categoría).

1. El "hash" de un archivo permite asegurarse de su integridad, para verificar que no fue modificado. Cuando se publican archivos de un leak, se suele publicar el hash también. Así, volver a calcular el hash (hay algoritmos y programas para esto) permite asegurarse que el archivo que uno tiene en las manos es el que se publicó originalmente.

¿Quién puede ayudar a entender este tipo de situaciones?

Si requiere comprender mejor las medidas que debe considerar para divulgar un incidente de seguridad digital, para manejar información de filtraciones o entender las implicaciones de estos casos, busque ayuda especializada.

Compartimos la información de las organizaciones que, en la región, pueden apoyar con este tipo de casos:

Laboratorio de seguridad digital de la Fundación Karisma ("K+Lab")
web: https://web.karisma.org.co/klab/
correo: klab@karisma.org.co

Línea de atención de Access Now:
https://www.accessnow.org/help-es/

Laboratorio de seguridad digital de Amnesty International ("Amnesty Tech"):
https://www.amnesty.org/en/tech/

Computer Incident Response Center for Civil Society:
https://www.civicert.org/

<K+LAB>



Participación cívica















karismacol @Karisma karismacol fundacionkarismaa

karisma.org.co